IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:

Want, et al.

Application No.: 10/025,088

Filed: December 18, 2001

For: Method and Device for Communicating Data

Examiner: Zewari, Sayed T.

Art Group: 2617

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDED APPEAL BRIEF
IN SUPPORT OF APPELLANT'S APPEAL
TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Sir:

Applicant (hereinafter "Appellant") hereby submits this Brief in support of its appeal from a final decision by the Examiner, mailed August 31, 2009, in the above-captioned case. Appellant respectfully requests consideration of this appeal by the Board of Patent Appeals and Interferences (hereinafter "Board") for allowance of the above-captioned patent application.

An oral hearing is not desired.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The invention is assigned to Intel Corporation, 2200 Mission College Boulevard, Santa Clara, California 95052, USA.

II. RELATED APPEALS AND INTERFERENCES

To the best of Appellant's knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision.

III. STATUS OF THE CLAIMS

Claims 1, 3-15 and 17-42 are currently pending in the above-referenced application. No claims have been allowed. Claims 2 and 16 have been cancelled. Thus, claims 1, 3-15 and 17-42 are the subject of this appeal.

IV. STATUS OF AMENDMENTS

In response to a Final Office Action, mailed on August 31, 2009, rejecting claims 1, 3-15 and 17-42, Appellant filed a Notice of Appeal on February 1, 2010.

A copy of all claims on appeal is attached hereto as an Appendix of Claims.

V. SUMMARY OF CLAIMED SUBJECT MATTER

In claim 1, a portable device is disclosed. The device includes a wireless communication module **(Figure 1, 24)** to communicate with each of a plurality of remote devices **(Figure 1, 14)** within a locality. **See Specification at page 4, lines 4-5 and page 5, lines 11-13.** The device further includes a data storage module **(Figure 1, 18)** having a public storage area **(Figure 1, 20)** with which selected remote devices exchange data in a free manner, and a private storage area **(Figure 1, 22)** with which selected remote devices exchange data in a restricted manner. **See Specification at page 4, lines 15-19 and page 11, lines 1-9.** Further, the device includes a controller **(Figure 1, 36)** connected to the wireless communication module **(Figure 1, 24)** and to the data storage module **(Figure 1, 18)** to establish a wireless communication link between the wireless communication module **(Figure 1, 24)** and a first remote device **(Figure 1, 14)** upon a determination that services offered by the first remote device are relevant and to grant access rights to the public storage area **(Figure 1, 20)** and the private storage area **(Figure 1, 22)**. **See Specification at page 4, lines 3-5, page 5, lines 1-5, page 9, lines 1-5 and 16-22 and page 10, lines 1-17.**

In claim 15, a data communication system includes a plurality of remote devices **(Figure 1, 14)**, where each remote device including a wireless communication interface **(Figure 1, 26)** and at least one portable device. **See Specification at page 4, lines 4-5 and page 5, lines 11-13.** The portable device includes a wireless communication module **(Figure 1, 24)** to communicate within a locality with the wireless communication interface **(Figure 1, 26)** the remote devices **(Figure 1, 14)**, a data storage module **(Figure 1, 18)** having a public storage area **(Figure 1, 20)** with which selected remote devices

exchange data in a free manner, and a private storage area **(Figure 1, 22)** with which selected remote devices exchange data in a restricted manner. **See Specification at page 4, lines 15-19 and page 11, lines 1-9.** The device also includes a controller **(Figure 1, 36)** connected to the wireless communication module **(Figure 1, 24)** and to the data storage module **(Figure 1, 18)** to establish a wireless communication link between the wireless communication module **(Figure 1, 24)** and a first remote device **(Figure 1, 14)** upon a determination that services offered by the first remote device are relevant and to grant access rights to the first remote device **(Figure 1, 14)** to the public storage area **(Figure 1, 20)** and the private storage area **(Figure 1, 22)**. **See Specification at page 4, lines 3-5, page 5, lines 1-5, page 9, lines 1-5 and 16-22 and page 10, lines 1-17.**

Claim 21 discloses a method. The method includes monitoring, by means of a portable device, wireless communications from a plurality of remote devices requesting communications with the portable device within a locality. **See Figure 3, 82 and Specification at page 8, lines 5-9.** The portable device includes a public storage area **(Figure 1, 20)** with which selected remote devices exchange data in a free manner and a private storage area **(Figure 1, 22)** with which selected remote devices exchange data in a restricted manner. **See Specification at page 4, lines 15-19 and page 11, lines 1-9.** The method also includes identifying access rights associated with the remote device. **See Figure 3, 98 and Specification at page 10, lines 2-5.** The method further establishes a wireless communication link between the wireless communication module **(Figure 1, 24)** and a first remote device **(Figure 1, 14)** upon a determination that services offered by the first remote device are relevant and grants access rights to the public storage area **(Figure 1, 18)** and the private storage area **(Figure 1, 22)** based on a classification of the first

remote device. **See Figure 3, 100, 102, 104 and 106 and Specification at page 10, line 6 – page 11, line 9.**

In claim 33, a computer program product is disclosed including a medium readable by a computer, the medium carrying instructions which, when executed by the computer, cause the computer **(See Figure 1 and Specification at page 4, lines 1-2)** to monitor wireless communications within a locality from a plurality of remote devices. **See Figure 3, 82 and Specification at page 8, lines 5-9.** Further to request substantive communications with a portable device **(Figure 1, 14)** including the processor **(Figure 1, 40)** and a data storage module **(Figure 1, 18)** a public storage area **(Figure 1, 20)** with which selected remote devices exchange data in a free manner and a private storage area **(Figure 1, 22)** with which selected remote devices exchange data in a restricted manner. **See Specification at page 4, lines 15-19 and page 11, lines 1-9.** The instructions further cause the computer to identify access rights associated with the remote device, **(See Figure 3, 98 and Specification at page 10, lines 2-5)** and to establish a wireless communication link between the wireless communication module **(Figure 1, 24)** and a first remote device **(Figure 1, 14)** upon a determination that services offered by the first remote device are relevant and grant access rights to the public storage area **(Figure 1, 18)** and the private storage area **(Figure 1, 22)** based on a classification of the first remote device. **See Figure 3, 100, 102, 104 and 106 and Specification at page 10, line 6 – page 11, line 9.**

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1, 3-8, 10-12, 15, 17-29 and 31-41 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Kiessling et al., U.S. 6,901,251 (hereinafter "*Kiessling*") in view of Proust et al., U.S. Patent No. 6,216,014 (hereinafter "*Proust*").

B. Claims 9, 13, and 42 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Kiessling* in view of Fifield, U.S. Patent No. 6,744,752 (hereinafter "*Fifield*").

C. Claims 14, 16 and 34 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Kiessling* in view of well-known prior art.

Rejections B and C are dependent on Rejection A. Therefore, Rejections B and C will not be discussed herein since the arguments will be identical to those presented against Rejection A.

VII. ARGUMENTS

1. THE PENDING CLAIMS WERE IMPROPERLY REJECTED UNDER 35 U.S.C. § 103(a) BECAUSE THE COMBINATION OF *KIESSLING* AND *PROUST* DO NOT DISCLOSE OR SUGGEST EACH AND EVERY FEATURE OF THE PENDING CLAIMS

Appellant respectfully submits that the combination of *Kiessling* and *Proust* fails to disclose or suggest the claimed invention for the reasons set forth below. As the Honorable Board is well aware, in order to establish a *prima facie* case of obviousness, the Office personnel must articulate the following:

> (1) a finding that the prior art included ***each element claimed***, although not necessarily in a single prior art reference, with the only difference between the claimed invention and the prior art being the lack of actual combination of the elements in a single prior art reference;
>
> (2) a finding that one of ordinary skill in the art could have combined the elements as claimed by known methods, and that in combination, each element merely performs the same function as it does separately;
>
> (3) a finding that one of ordinary skill in the art would have recognized that the results of the combination were predictable; and
>
> (4) whatever additional findings based on the *Graham* factual inquiries may be necessary, in view of the facts of the case under consideration, to explain a conclusion of obviousness. (emphasis added)

Manual of Patent Examining Procedure (MPEP), 8th Edition, Revision 6, September 2007, §2143 (A).

(A) **Claims 1, 3-8, 10-12, 15, 17-29 and 31-41 were improperly rejected because the combination of *Kiessling* and *Proust* does not disclose or suggest a controller to establish a wireless communication link between the wireless communication module and a first remote device upon a determination that services offered by the first remote device are relevant and to grant access rights to the public storage area and the private storage area based on a classification of the first remote device.**

Claims 1, 3-8, 10-12, 15, 17-29 and 31-41 are patentable in view of *Kiessling* and *Proust* under 35 U.S.C. § 103(a). For example, Appellant's claim 1 recites:

> A portable device, which includes:
> a wireless communication module to communicate with each of a plurality of remote devices within a locality;
> a data storage module having a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner; and
> a controller connected to the wireless communication module and to the data storage module, to establish a wireless communication link between the wireless communication module and a first remote device upon a determination that services offered by the first remote device are relevant and to grant access rights to the public storage area and the private storage area based on a classification of the first remote device.

Appellant's claim 15 recites:

> A data communication system, which includes:
> a plurality of remote devices, each remote device including a wireless communication interface; and
> at least one portable device, which includes:
> a wireless communication module to communicate within a locality with the wireless communication interface the remote devices;
> a data storage module having a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner; and
> a controller connected to the wireless communication module and to the data storage module, to establish a wireless communication link between the wireless communication module and a first remote device upon a determination that services offered by the first remote device are relevant and to grant access rights to the public storage area and the private storage area based on a classification of the first remote device.

Appellant's claim 21 recites:

> A method which includes:
> monitoring, by means of a portable device, wireless communications from a plurality of remote devices requesting communications with the portable device within a locality, the portable device including a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner;
> identifying access rights associated with the remote device; and
> establishing a wireless communication link between the wireless communication module and a first remote device upon a determination that services offered by the first remote device are relevant; and
> granting access rights to the public storage area and the private storage area based on a classification of the first remote device.

Appellant's claim 33 recites:

> A computer program product including a medium readable by a computer, the medium carrying instructions which, when executed by the computer, cause the computer to:
> monitor wireless communications within a locality from a plurality of remote devices requesting substantive communications with a portable device including the processor and a data storage module a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner;
> identify access rights associated with the remote device; and
> establishing a wireless communication link between the wireless communication module and a first remote device upon a determination that services offered by the first remote device are relevant; and
> granting access rights to the public storage area and the private storage area based on a classification of the first remote device.

Kiessling discloses a mobile telephone capable of serving an external application, which is located in a remote device. Such an external application will communicate with the mobile telephone over a wireless link (i.e., radio, short-range supplementary data or infrared). The user will interact with the external application through the man-machine interface of the mobile telephone. See *Kiessling* at col. 5, ll. 32-40. The mobile telephone includes a controller, an operating system a local storage device for storing a first application, a secure resource that is only accessible from the operation system and a wireless interface for connecting the mobile telephone to the remote device. *Kiessling* at col. 1, ll. 15-21 and col. 4, ll. 15-18.

Proust discloses a data storage having a plurality of files. Each of these files is associated with a standard access control policy. This is defined by a plurality of standard access conditions (AC standard), each applying to a separate command that can access this file. See *Proust* at col. 11, ll. 14-18.

Appellant submits that neither *Kiessling* nor *Proust* disclose or suggest a controller granting access rights to a public storage area and a private storage area based on a classification of a remote device. However, the Examiner cites *Proust* as disclosing this feature since *Proust* discloses that selected remote devices exchange data in a restricted manner. See Final Office Action at Page 5, lines 8-11. Notwithstanding the Examiner's assertion, there is no disclosure in *Proust* of a process of *granting access rights to a public storage area and a private storage area* ***based on a classification of a remote device***.

The Examiner further asserts that such an argument against *Proust* is not valid since "one cannot show non-obviousness by attacking references individually where the

rejections are based on combinations of references." See Final Office Action at Page 3, lines 13-15. Appellant respectfully disagrees with the Examiner's assertion since Appellant maintains that neither reference, alone or in combination, suggests the recited element of the claims. Moreover, Appellant's argument against *Proust* is made to dispute the Examiner's reference of *Proust* as disclosing a process of *granting access rights to a public storage area and a private storage area* ***based on a classification of a first remote device***.

Since neither *Kiessling* nor *Proust* disclose or suggest a controller to establish a wireless communication link between the wireless communication module and a first remote device upon a determination that services offered by the first remote device are relevant and to grant access rights to the public storage area and the private storage area based on a classification of the first remote device, any combination of *Kiessling* and *Proust* would disclose or suggest such a feature. Consequently, the Examiner has not established a prima facie case of obviousness.

Claims 3-14 depend from claim 1, claims 17-20 depend from claim 15, claims 22-31 depend from claim 21 and claims 33-42 depend from claim 32. Given that dependent claims necessarily include the limitations of the claims from which they depend, Appellant submits that the invention as claimed in claims 3-14, 17-20, 22-31 and 33-42 are similarly patentable over the combination of *Kiessling* and *Proust*.

For the forgoing reasons, Appellant submits that the Examiner has failed to search and find a printed publication or patent that discloses the claimed invention as set forth in MPEP § 706.02(a).

Thus, the Examiner erred in rejecting claims 1, 3-15 and 17-42 under 35 U.S.C. § 103(a).

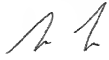
VIII. CONCLUSION

Appellant respectfully submits that all the appealed claims in this application are patentable and request that the Board of Patent Appeals and Interferences overrule the Examiner and direct allowance of the rejected claims.

This brief is submitted, along with a check for $540.00 to cover the appeal fee for one other than a small entity as specified in 37 C.F.R. § 1.17(c). Please charge any shortages and credit any overpayment to out Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN



Date: 2/9/10

Mark L. Watson
Attorney for Appellant
Reg. No. 46,322

1279 Oakmead Parkway
Sunnyvale, California 94085-4040
(303) 740-1980

IX. APPENDIX OF CLAIMS (37 C.F.R. § 1.192(c)(9))

1. A portable device, which includes:

a wireless communication module to communicate with each of a plurality of remote devices within a locality;

a data storage module having a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner; and

a controller connected to the wireless communication module and to the data storage module, to establish a wireless communication link between the wireless communication module and a first remote device upon a determination that services offered by the first remote device are relevant and to grant access rights to the public storage area and the private storage area based on a classification of the first remote device.

3. A portable device as claimed in Claim 1, in which the controller filters requests from each of the remote devices to exchange data and to reject and accept the requests in response to the nature of services offered by the remote device.

4. A portable device as claimed in Claim 1, in which the controller defines access rights to the first and second storage areas and, dependent upon the access rights, allows the remote device to store and retrieve data from at least one of the first and second storage areas.

5. A portable device as claimed in Claim 1, in which a digital certificate of authenticity is requested from the remote device prior to communicating data between the remote device and the private storage area.

6. A portable device as claimed in Claim 1, in which the controller restricts how often and the amount of data which is writable by the remote device into the public storage area.

4. A portable device as claimed in Claim 1, in which data stored in the public storage area is selectively cleared by the controller in an automated fashion.

5. A portable device as claimed in Claim 1, in which the portable device and the remote device communicate using secure sockets layer (SSL) protocols.

6. A portable device as claimed in Claim 1, which detects Universal Plug and Play (UPnP) broadcasts.

7. A portable device as claimed in Claim 1, in which the wireless communication module is a radio frequency (RF) transceiver which communicates using a standardized communication protocol.

8. A portable device as claimed in Claim 10, in which the standardized communication protocol is selected from the group including Bluetooth IEEE 802.15 technology, IEEE 802.11a technology, and IEEE 802.11b technology.

9. A portable device as claimed in Claim 1, in which the controller interfaces the portable device to a computer system to permit a user to access and store data in the data storage module.

10. A device as claimed in Claim 1, in which the remote device is defined by another portable device within the locality.

11. A device as claimed in Claim 1, which includes a rechargeable power supply for powering its various components.

12. A data communication system, which includes:

a plurality of remote devices, each remote device including a wireless communication interface; and

at least one portable device, which includes:

a wireless communication module to communicate within a locality with the wireless communication interface the remote devices;

a data storage module having a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner; and

a controller connected to the wireless communication module and to the data storage module, to establish a wireless communication link between the wireless communication module and a first remote device upon a determination that services offered by the first remote device are relevant and to grant access rights to the public storage area and the private storage area based on a classification of the first remote device.

14. A system as claimed in Claim 15, in which the controller filters requests from each of the remote devices to exchange data and to selectively reject and accept the requests in response to the nature of services offered by the remote device.

15. A system as claimed in Claim 15, in which the controller defines access rights to the first and second storage areas and, dependent upon the access rights, allows the remote device to store and retrieve data from at least one of the first and second storage areas.

16. A system as claimed in Claim 15, in which a digital certificate of authenticity is requested from the remote device prior to communicating data between the remote device and the private storage area.

17. A system as claimed in Claim 15, in which the controller restricts the amount of data which is writable by the remote device into the public storage area.

18. A method which includes:

monitoring, by means of a portable device, wireless communications from a plurality of remote devices requesting communications with the portable device within a locality, the portable device including a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner;

identifying access rights associated with the remote device; and

establishing a wireless communication link between the wireless communication module and a first remote device upon a determination that services offered by the first remote device are relevant; and

granting access rights to the public storage area and the private storage area based on a classification of the first remote device.

19. A method as claimed in Claim 21, which includes exchanging data in a relatively free manner between the first storage area, which defines a public data storage area, and the remote device, and exchanging data in a relatively restricted manner between the second storage area, which defines a private data storage area, and the remote device.

20. A method as claimed in Claim 21, which includes:

filtering requests for substantive communications from each of the remote devices with the portable device ; and

selectively rejecting and accepting the requests in response to the nature of services offered by the remote device.

21. A method as claimed in Claim 22, which includes defining access rights to the first and second storage areas and, dependent upon the access rights, allowing the remote device to store and retrieve data from at least one of the first and second storage areas.

22. A method as claimed in Claim 24, in which the access rights are dependent upon a classification of the remote device by the portable device.

23. A method as claimed in Claim 22, which includes requesting a digital certificate of authenticity from the remote device prior to communicating data between the remote device and the private storage area.

24. A method as claimed in Claim 22, which includes restricting the amount of data which is writable by the remote devices into the public storage area.

25. A method as claimed in Claim 22, which includes selectively clearing data in the public storage area.

26. A method as claimed in Claim 21, which includes communicating between the portable device and the remote device using secure sockets layer (SSL) protocols.

27. A method as claimed in Claim 21, which includes detecting universal plug and play (UPnP) broadcasts from each remote device.

28. A method as claimed in Claim 21, which includes communicating via a radio frequency (RF) transceiver using a standardized communication protocol.

29. A method as claimed in Claim 31, which includes communicating using technology selected from the group including Bluetooth 802.15 technology, IEEE 802.11a technology and IEEE 802.11b technology.

30. A computer program product including a medium readable by a computer, the medium carrying instructions which, when executed by the computer, cause the computer to:

monitor wireless communications within a locality from a plurality of remote devices requesting substantive communications with a portable device including the processor and a data storage module a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner;

identify access rights associated with the remote device; and

establishing a wireless communication link between the wireless communication module and a first remote device upon a determination that services offered by the first remote device are relevant; and

granting access rights to the public storage area and the private storage area based on a classification of the first remote device.

31. A computer program product as claimed in Claim 33, in which data is exchanged in a relatively free manner between the first storage area, which defines a public data

storage area, and the remote device, and data is exchanged in a relatively restricted manner between the second storage area, which defines a private data storage area, and the remote device.

32. A computer product as claimed in Claim 33, in which requests for substantive communications from each of the remote devices with the portable device are filtered, the requests being selectively rejected and accepted in response to the nature of services offered by the remote device.

33. A computer program product as claimed in Claim 33, which includes defining access rights to the first and second storage areas and, dependent upon the access rights, allowing the remote device to store and retrieve data from at least one of the first and second storage areas.

34. A computer program product as claimed in Claim 36, in which the access rights are dependent upon the classification of the remote device by the portable device.

35. A computer program product as claimed in Claim 34, which includes requesting a digital certificate of authenticity from the remote device prior to communicating data between the remote device and the private storage area.

36. A computer program product as claimed in Claim 34, which includes restricting how often and the amount of data which is writable by the remote devices into the public storage area.

37. A computer program product as claimed in Claim 34, which includes selectively clearing data in the public area.

38. A computer program product as claimed in Claim 33, which includes communicating between the portable device and the remote device using secure sockets layer (SSL) protocols.

42. A computer program product as claimed in Claim 33, which includes detecting universal plug and play (UPnP) broadcasts from each remote device.

X. EVIDENCE APPENDIX

None.

XI. RELATED PROCEEDINGS APPENDIX

None.